Don't Be Maxed Out by Identity Theft!

January 2007 - Cyber Security

Are you exposing information and increasing your vulnerability to identity theft?

- Do you put paycheck stubs or old forms containing confidential information in the garbage at work?
- Do you enter personal information in online registration forms?
- Do you infrequently (or never) scan your computer for spyware?

If you answered "yes" to any or all of these questions, you should take immediate steps to protect your most valuable asset--your identity! Incidents of identity theft have steadily increased since 2001, according to the Federal Trade Commission (FTC), which cites identity theft as the number one concern of consumers contacting it for information or to file complaints.

How Is Identity Stolen?

Identity thieves employ a variety of means to steal private information for their own use. They may hack into large computer databases that contain confidential information, use spyware to intercept communications from individual computers, physically steal personal or financial documents from garbage cans, or trick unsuspecting individuals into disclosing private information over the telephone or online.

Do's and Don't for Preventing Identity Theft

- **DO** protect your computer from hackers and spyware. Use an active firewall and current antivirus and anti-spyware programs to protect yourself and your computer when you're online.
- **DO** have a security mindset! Always be skeptical of unfamiliar sites and links, and of suspicious e-mail and IM messages.
- **DO** dispose of confidential information properly. Shred paper documents and use a disk cleaning program on computers and portable devices before you dispose of them.
- **DO** check your credit reports regularly for signs of suspicious activity.
- **DON'T** post personal information on Web sites or in chat rooms.
- **DON'T** enter more information than is absolutely necessary in online registration forms or give unnecessary information, such as your Social Security number, to businesses or retailers.
- **DON'T** visit Web sites using third party links. Open a new browser and type the address yourself if you want to visit a site.
- **DON'T** fall for phishing scams! Never reply to phone calls, e-mail, or pop-up messages asking for personal or financial information.
- **DON'T** share passwords or account PINs with anyone.

If You Suspect You Are a Victim of Identity Theft:

- File a report with the local police department. To report incidents on campus, call University Police (UP) at extension 456 from any campus phone. From outside the University, call UP at (847) 491-3456 (Evanston) or (312) 503-3456 (Chicago).
- Visit the FTC's Identity Theft Web site to get information about contacting credit bureaus, closing accounts, and filing complaints.